Lecture 3 Image Classification

IMAGE PROCESSING AND COMPUTER VISION - PART 2 SAMUELE SALTI

Image Classification

Input



Output

Choose among these categories

Dog

Cat

Bird

Frog

Person

Some challenges



Intraclass variations



Viewpoint variations



Background clutter



Illumination changes



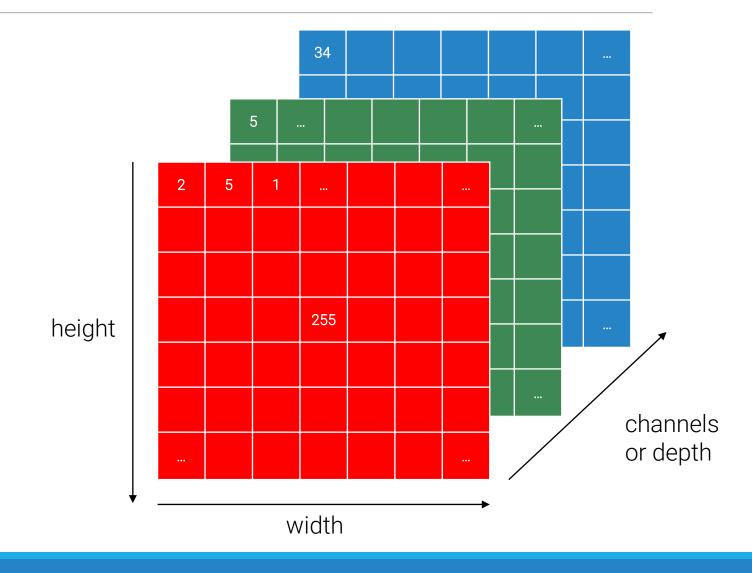
Occlusions



General weirdness of the world...

RGB images are tensors in a computer





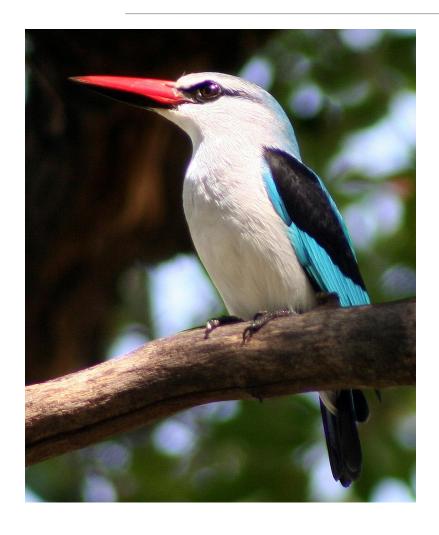
Categories as numbers



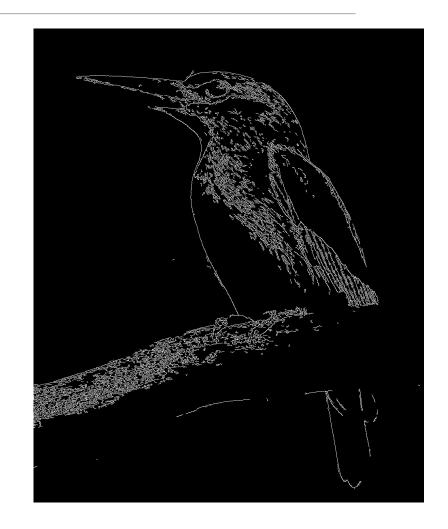
) = 2

0 -> Dog
1 -> Cat
2 -> Bird
3 -> Frog
4 -> Person

How far can «classic» computer vision bring us?



detect_edges(image)
If ???

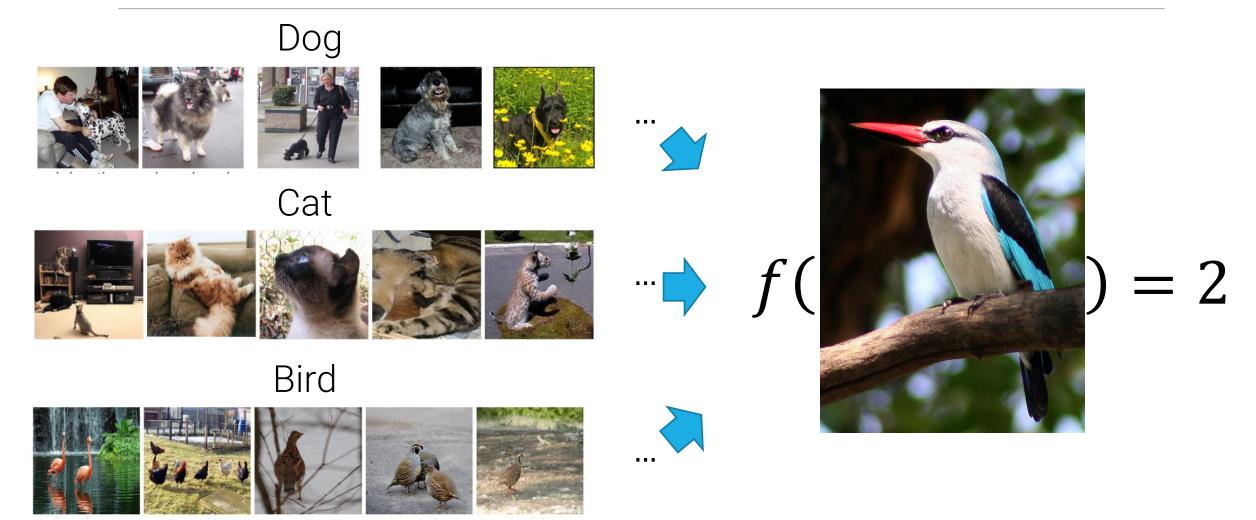


Birds...



Traditional Computer Vision techniques, e.g. handcrafted rules based on edges, need a controlled environment, usually feasible in industrial vision applications, otherwise they are very brittle.

(Supervised) Machine learning to the rescue



Training and testing dataset

When applying machine learning methods, we are given (or we create):

- o a training set $D^{train} = \{ (x^{(i)}, y^{(i)}) | i = 1, ..., N \}$
- o a test set $D^{test} = \{ (x^{(i)}, y^{(i)}) | i = 1, ..., M \}$

where $\mathbf{x}^{(i)} \in \mathbb{R}^f$, are the features representing the real word **items** we care about (i.e. images in our case), and $y^{(i)}$ are the outputs we want to predict for that item, i.e. the **label** in image classification.

We assume the two sets contains independent and identically distributed samples from the **same** unknown distribution $p_{data}(x, y)$

The place in which we extract a dataset about also an object really makes the difference and puts a gap if compared with other nations (ex. bottles in USA vs Argentina)

Modified NIST (MNIST)

10 classes: handwritten digits from 0 to 9

50k train images

10k test images

28x28 grayscale images

Results on MNIST may not generalize to other datasets

CIFAR 10

airplane
automobile
bird
cat
deer
dog

Subset of the 80 million Tiny Images dataset

https://www.cs.toronto.edu/~kriz/cifar.ht ml

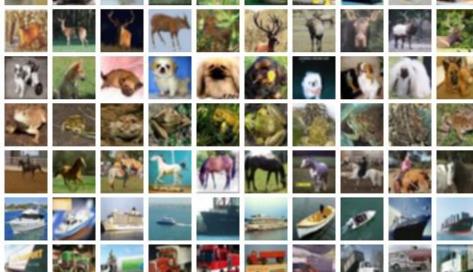
10 classes

50k training images

10k testing images

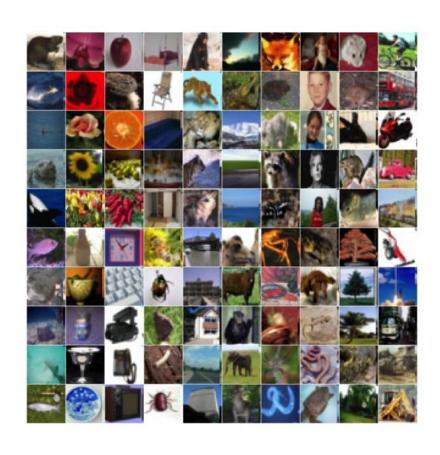
32x32 RGB images

frog horse ship truck



Learning Multiple Layers of Features from Tiny Images, Alex Krizhevsky, 2009.

CIFAR 100



Another subset of the 80 million Tiny Images dataset

100 classes

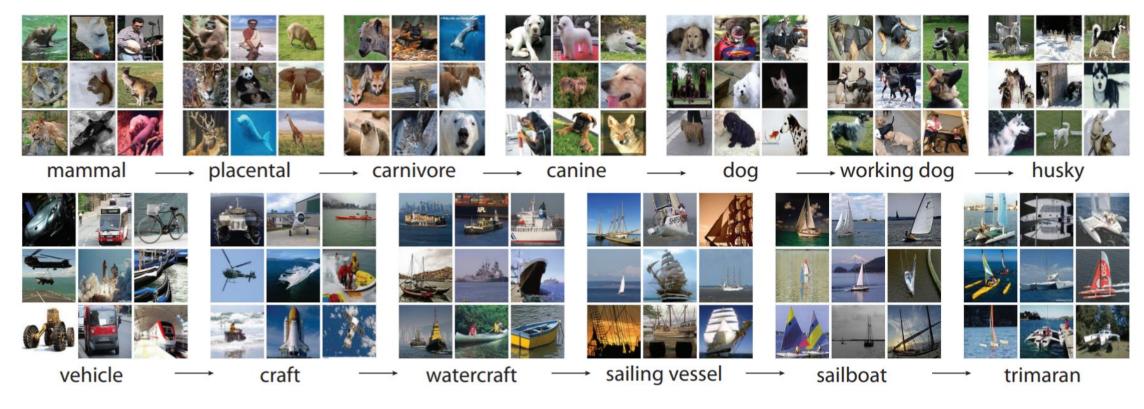
50k training images (500 per class)

10k testing images (100 per class)

32x32 RGB images

Hierarchical structure: 20 super-classes with 5 subclasses each

ImageNet / ImageNet 21k



14 millions RGB images at full and variable resolution with average size about 400×350 .

Hierarchical structure: modelled on about 21k synsets from WordNet (out of 50k)

ILSVRC – often referred to as ImageNet / ImageNet1k

Image classification

Easiest classes

goldfinch (100) flat-coated retriever (100) red fox (100) hen-of-the-woods (100) ibex (100)











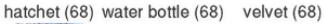
hamster (100)



Hardest classes

muzzle (71)









loupe (66)





ladle (65)







hook (66)









1000 classes

1.3M training images (about 1300 per class)

50k validation images (50 per class)

100k test images (100 per class)

Variable resolution RGB images as in ImageNet, often resized to 256x256 for training.

Due to the inherent ambiguity of assigning only one label to each image, performance is usually reported as top-5 accuracy: an image is considered correctly classified if the correct label is present in 5 classes predicted by the algorithm. Multi-label accuracy has also been recently proposed

https://cs.stanford.edu/people/karpathy/ilsvrc/

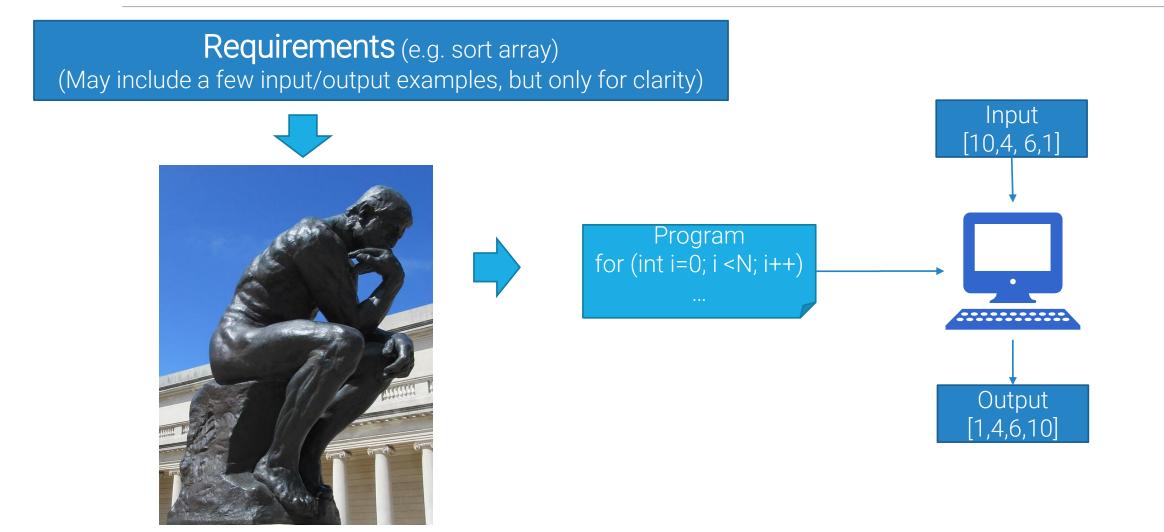
Russakovsky et al, "ImageNet Large Scale Visual Recognition Challenge", IJCV 2015 Vaishaal Shankar et al., Evaluating Machine Accuracy on ImageNet, ICML 2020

And many more...

A great resource to find datasets together with state-of-the-art methods is https://paperswithcode.com/sota

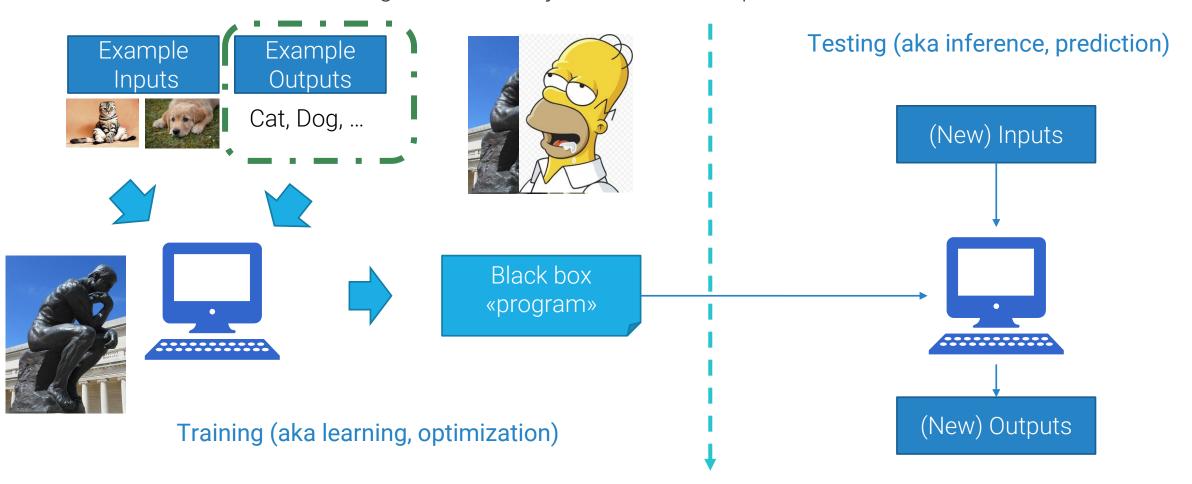
Benchr	marks					• Add a Result
TREND	DATASET	BEST METHOD	PAPER TITLE	PAPER	CODE	COMPARE
20 20 20 20 20 20 20	ImageNet	FixEfficientNet-L2	Fixing the train-test resolution discrepancy: FixEfficientNet	L	O	See all
Di Di Di Di Di Di Di Di	CIFAR-10	P BiT-L (ResNet)	Big Transfer (BiT): General Visual Representation Learning	L	0	See all
20 20 20 20 20 20 20	CIFAR-100	P BiT-L (ResNet)	Big Transfer (BiT): General Visual Representation Learning	L	0	See all
20 20 20 20 20 20 20	MNIST	Branching/Merging CNNHomogeneous FilterCapsules	A Branching and Merging Convolutional Network with Homogeneous Filter Capsules	L	0	See all
2 20 20 20 20 20 20 20	SVHN	Ÿ WideResNet-28-10	RandAugment: Practical automated data augmentation with a reduced search space	6	O	See all
20 20 20 20 20 20 20	STL-10	₹ NAT-M4	Neural Architecture Transfer	•	0	See all

A bird's eye view of traditional programming



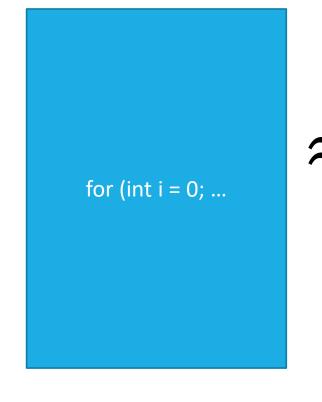
Machine learning or data-driven approach

We can think of machine learning as a new way to instruct computers about what we want them to do.

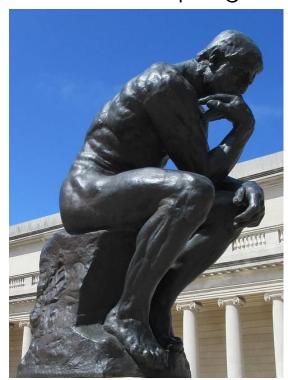


Data-driven approach: other consequences

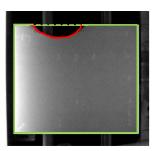
The rise of data-driven approaches changes the relative importance of data and algorithms







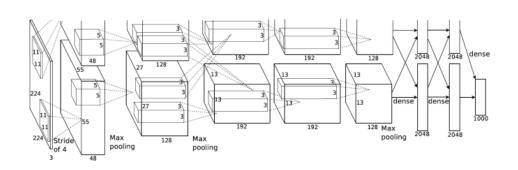




Data-driven approach: other consequences

Data and datasets are crucial in this new paradigm. To know the most used ones for each vision task and to understand the impact of metrics on the results is therefore at least as important as it is to know the latest and greatest machine learning models.

Data-driven approach





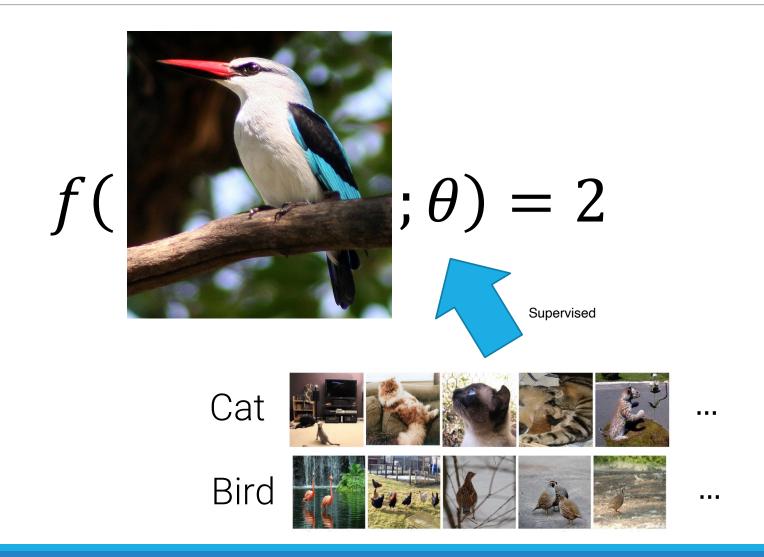
MLOps: From Model-centric to Data-centric Al



"If 80% of machine learning is data preparation, we should invest more in it and be more systematic about it"

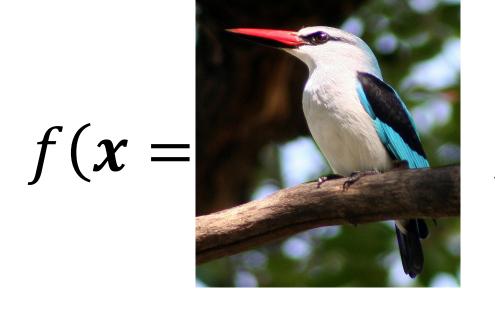


Parametric approach



Linear classifier

But numbers are simply numbers and they can chage as they are in a lookup table

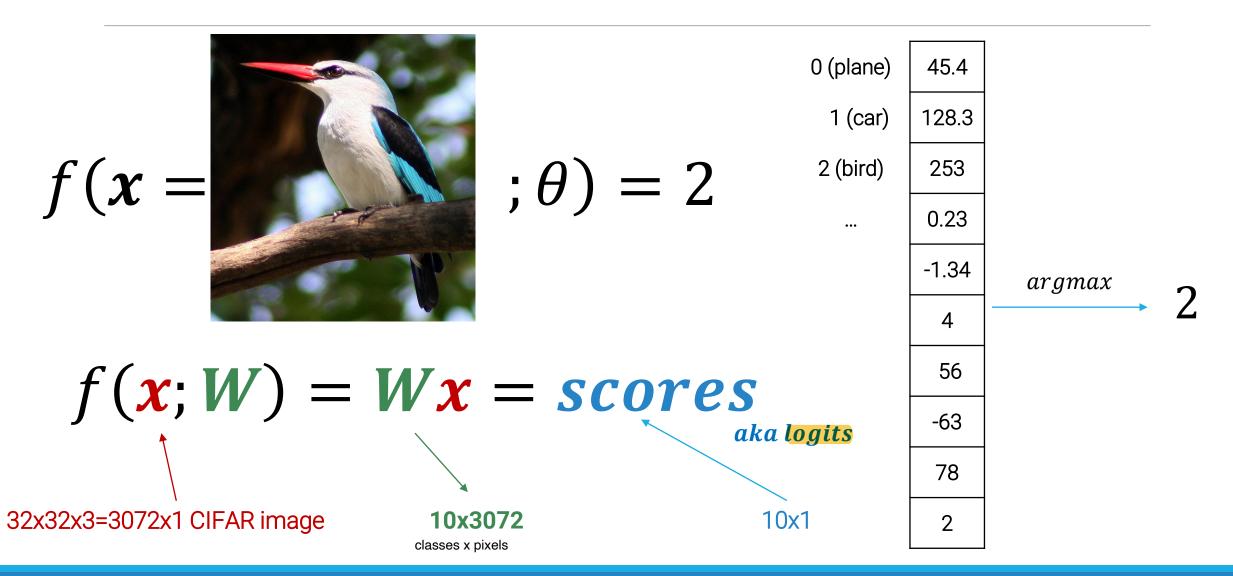


$$;\theta)=2$$

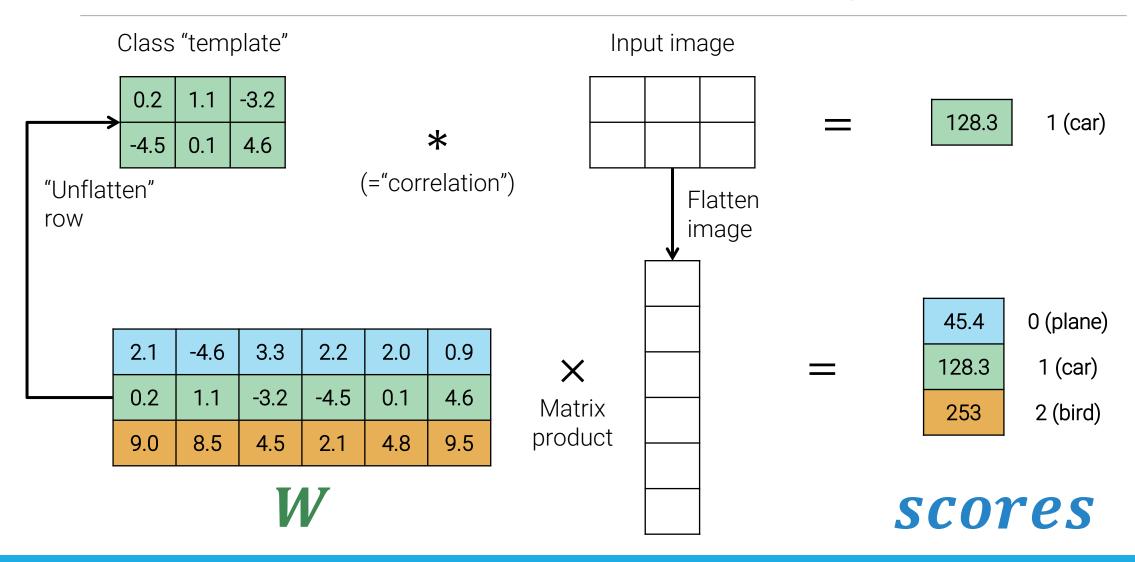
$$f(x; W) = Wx = class$$
32x32x3=3072x1 CIFAR image 1x3072 Scalar

idea! Bad Classes are categorical variables, their assignment to integer ids is random and it is not designed to capture the semantic of classes (i.e. if cat is class 3 and we get class=2,5 out of f, it does not mean that xdepicts half a bird and half a cat; or, similarly, the fact that two ids are nearby or far away does not mean that the corresponding classes share or not visual similarities)

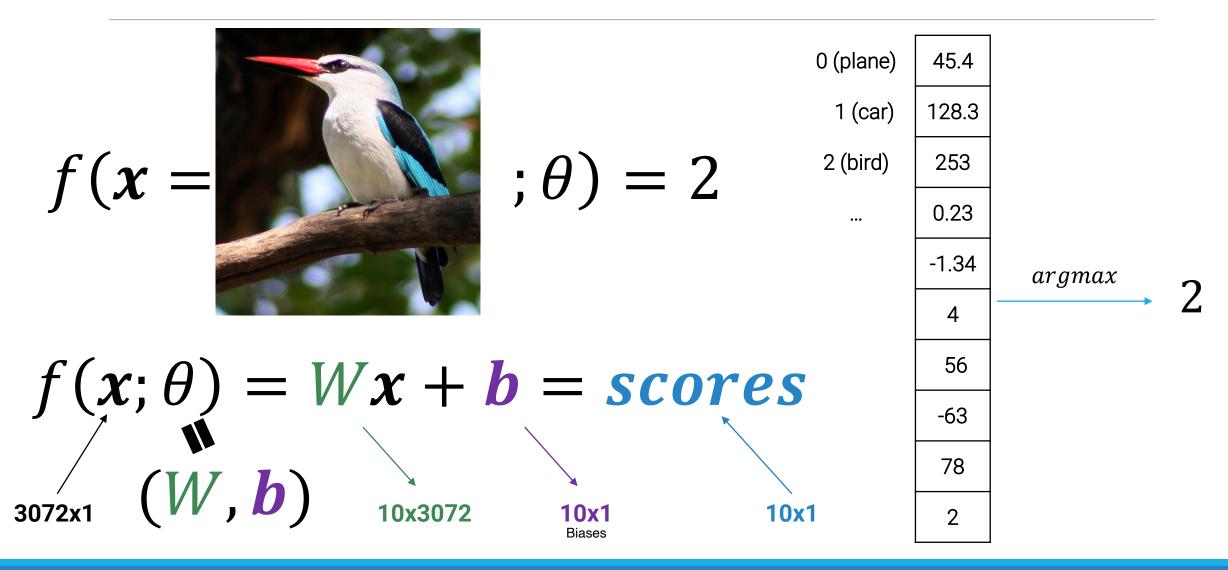
Linear classifier



Linear classifier as "template matching"



In ML, linear often means affine...



Learning as optimization

The space of the functions that a machine learning model can produce is its **hypothesis space** H

Learning = solve an **optimization problem** to find the "best" **function** $h \in \mathbb{H}$

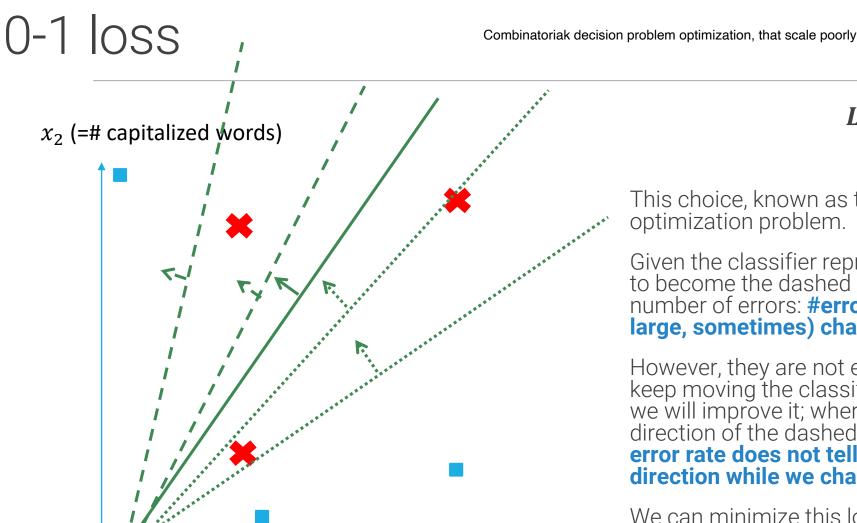
$$h^* = \operatorname{argmin}_{h \in \mathbb{H}} L(h, D^{train})$$

Parametric models

Learning = solve an **optimization problem** to find the "best" **parameters** $\theta \in \Theta$

$$\theta^* = \operatorname{argmin}_{\theta \in \Theta} L(\theta, D^{train})$$

What function *L* should we minimize?



 x_1 (=#urls)

$$L = \#errors?$$

This choice, known as the **0-1 loss**, results in a hard optimization problem.

Given the classifier represented by the solid line, changing it to become the dashed or the dotted line produces the same number of errors: #errors is insensitive to small (and even large, sometimes) changes of the parameters.

However, they are not equivalent directions of change: if we keep moving the classifier in the direction of the dotted line, we will improve it; whereas, if we keep moving in the direction of the dashed one, we will make more errors: the error rate does not tell us if we are "moving" in the "right" direction while we change the parameters.

We can minimize this loss as a combinatorial optimization problem, but then it does not scale well to large datasets

The loss function

Instead of directly optimizing accuracy, we then usually optimize a proxy measure, the **loss** function, that is **easier to optimize but still correlated with how good our classifier is**.

Loss function is also called **objective function**, **cost function**, **error function**,...

If the loss is high, our classifier is performing poorly, and we also expect low accuracy.

If the loss is low, our classifier is good, and we also expect high accuracy.

Hence, we prefer values of the parameters that minimize it on the training set

$$\theta^* = \operatorname{argmin}_{\theta \in \Theta} L(\theta, D^{train})$$

We will always work with losses whose value on a dataset is the average (or the sum) of the values for the single samples

$$L(\theta, D^{train}) = \frac{1}{N} \sum_{i} L(\theta, (x^{(i)}, y^{(i)}))$$

What loss can we use for the linear classifier?

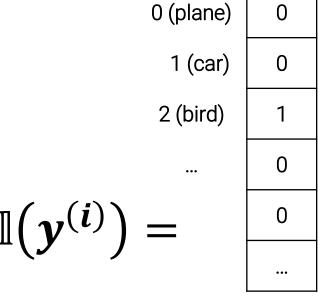
Historically, the RMSE between the prediction and the training label was used

$$L(\theta, (x^{(i)}, y^{(i)})) = L(Wx^{(i)} + b, y^{(i)}) = ||Wx^{(i)} + b - 1(y^{(i)})||_2$$



 $f(\mathbf{x}^{(i)};\theta) = W\mathbf{x}^{(i)} + \mathbf{b} =$

0 (plane)	45.4		
1 (car)	128		
2 (bird)	253		
•••	0.23		
_	-1.34		



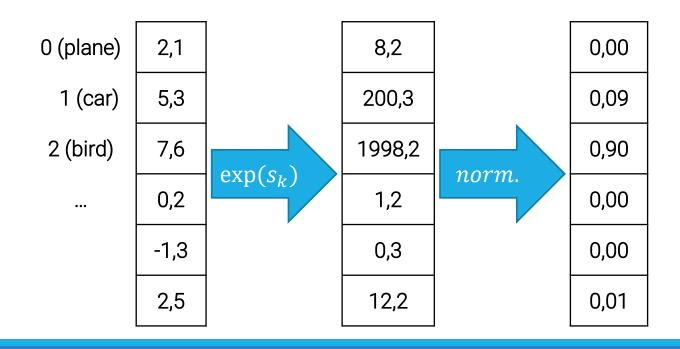
This is called one-hot encoding of class bird

Softmax function

It turns out there are theoretical and practical reasons to prefer a loss that transforms the scores computed by the classifier into probabilities and then perform maximum likelihood estimation of θ .

How do we go from scores s_i to probabilities? We use the **softmax** function (**softmax**: $\mathbb{R}^n \to \mathbb{R}^n$)

$$p_{model}(Y = j | X = x^{(i)}; \theta) = \operatorname{softmax}_{j}(s) = \frac{\exp(s_{j})}{\sum_{k=1}^{C} \exp(s_{k})}$$



Should be called "softargmax", as it is a smooth and differentiable approximation of the one-hot encoding of the *argmax*

To implement it reducing numerical issues, it is useful to note that

$$\operatorname{softmax}_{j}(s+c) = \frac{\exp(s_{j}+c)}{\sum_{k} \exp(s_{k}+c)} = \frac{\exp(s_{j})\exp(c)}{\sum_{k} \exp(s_{k})\exp(c)} = \frac{\exp(c)\exp(s_{j})}{\exp(c)\sum_{k} \exp(s_{k})} = \operatorname{softmax}_{j}(s)$$

and then compute it as $\operatorname{softmax}\left(s - \max_{k} s_{k}\right)$

Cross-entropy loss

Now that our linear classifier outputs «probabilities» over the classes, we can think of it as **a family of probability mass functions** over the classes given an image, indexed by the vector of parameters θ

$$\operatorname{softmax}\left(f\left(\boldsymbol{x}^{(i)};\theta\right)\right) \doteq p_{model}(Y | \boldsymbol{X} = \boldsymbol{x}^{(i)};\theta)$$

Then, the maximum likelihood estimation of θ is

0 (plane) 0,00
1 (car) 0,09
2 (bird) 0,90
... 0,00
0,00
0,01

$$\theta^* = \arg\max_{\theta} p_{model} \left(y^{(1)}, \dots, y^{(N)} \middle| \mathbf{x}^{(1)}, \dots, \mathbf{x}^{(N)}; \boldsymbol{\theta} \right)$$

$$= \arg\max_{\theta} \prod_{i=1}^{N} p_{model} \left(Y = y^{(i)} \middle| \mathbf{X} = \mathbf{x}^{(i)}; \boldsymbol{\theta} \right)$$

$$= \arg\max_{\theta} \sum_{i=1}^{N} \log p_{model} \left(Y = y^{(i)} \middle| \mathbf{X} = \mathbf{x}^{(i)}; \boldsymbol{\theta} \right)$$

$$= \arg\min_{\theta} \sum_{i=1}^{N} -\log p_{model} \left(Y = y^{(i)} \middle| \mathbf{X} = \mathbf{x}^{(i)}; \boldsymbol{\theta} \right)$$

Avoid the «curse of products»

i.i.d. data

Per-sample cross-entropy loss $L(\theta, (x^{(i)}, y^{(i)}))$

If the true class of this image is "bird", then the cross-entropy loss is $-\log(0.9) = 0.1$ (low value) If it were "car", then the loss value would have been $-\log(0.09) = 2.4$ (high value)

Putting everything together

Given

$$p_{model}(Y = j | X = x^{(i)}; \theta) = \operatorname{softmax}_{j}(s) = \frac{\exp(s_{j})}{\sum_{k=1}^{C} \exp(s_{k})}$$

and the per-sample loss to minimize to perform maximum likelihood estimation

$$-\log p_{model}\left(Y=y^{(i)} \mid X=x^{(i)}; \boldsymbol{\theta}\right)$$

the overall expression for the per-sample loss becomes

$$-\log\left(\frac{\exp\left(s_{\mathbf{y}^{(i)}}\right)}{\sum_{k=1}^{C}\exp\left(s_{k}\right)}\right) = -\log\left(\exp\left(s_{\mathbf{y}^{(i)}}\right)\right) + \log\left(\sum_{k=1}^{C}\exp\left(s_{k}\right)\right) = -s_{\mathbf{y}^{(i)}} + \log\left(\sum_{k=1}^{C}\exp\left(s_{k}\right)\right)$$

The second term of the sum on the right is usually referred to as the logsumexp and numerical libraries (e.g. PyTorch) usually have numerically stable functions to compute it. It approximates the max function, hence we can think of the cross-entropy loss as approximately

$$-\log\left(\frac{\exp(s_{\mathbf{y}(i)})}{\sum_{k=1}^{C}\exp(s_k)}\right) \approx -s_{\mathbf{y}(i)} + \max_{k} s_k$$

and of minimizing it as penalizing the most active incorrect prediction, i.e. a proxy to increase accuracy.

Losses in PyTorch

In PyTorch, you will find both NLLLoss (where NLL stands for negative log likelihood) and CrossEntropyLoss. Pay attention to the difference!

```
CLASS torch.nn.CrossEntropyLoss(weight: Optional[torch.Tensor] = None, size_average=None, ignore_index: int = -100, reduce=None, reduction: str = 'mean') [SOURCE]
```

This criterion combines nn.LogSoftmax() and nn.NLLLoss() in one single class.

It is useful when training a classification problem with C classes. If provided, the optional argument weight should be a 1D Tensor assigning weight to each of the classes. This is particularly useful when you have an unbalanced training set.

The input is expected to contain raw, unnormalized scores for each class.

input has to be a Tensor of size either (minibatch, C) or (minibatch, C, d), of

```
CLASS torch.nn.NLLLoss(weight: Optional[torch.Tensor] = None, size_average=None, ignore_index: int = -100, reduce=None, reduction: str = 'mean') [SOURCE]
```

The negative log likelihood loss. It is useful to train a classification problem with C classes.

If provided, the optional argument weight should be a 1D Tensor assigning weight to each of the classes. This is particularly useful when you have an unbalanced training set.

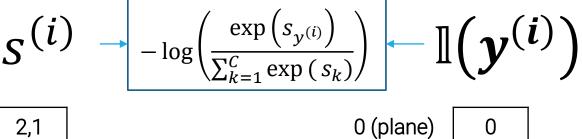
The input given through a forward call is expected to contain log-probabilities of each class. input has to be a Tensor of size either (minipatch, C) or (minipatch, C, $\alpha_1, \alpha_2, ..., \alpha_K$) with $K \geq 1$ for the K-dimensional case (described later).

Obtaining log-probabilities in a neural network is easily achieved by adding a LogSoftmax layer in the last layer of your network. You may use CrossEntropyLoss instead, if you prefer not to add an extra layer.

The target that this loss expects should be a class index in the range [0, C-1] where C = number of classes; if

Where are we?





1 (car)

0 (plane) 2,1 1 (car) 5,3 2 (bird) 7,6 ... 0,2 -1,3

2,5

3,5

4,5

5,5

6,5

Now we can express preferences over different choices of θ with one number. How can we use this knowledge to train our model, i.e. select the "best" θ ?

f(x)	$(i); \theta$ =	Wx +	b =
	(W, \boldsymbol{b})		
3072x1		10x3072	10x1

Gradient descent

$$\theta^* = argmin_{\theta \in \Theta} \sum_{i} L(\theta, (x^{(i)}, y^{(i)}))$$

0. (Randomly) initialize $\theta^{(0)}$

for e = 1, ..., E epochs

- 1. Forward pass: classify all the training data to get the predictions $\hat{y}^{(i)} = f(x^{(i)}; \theta^{(e-1)})$ and the loss $L(\theta^{(e-1)}, D^{train})$
- 2. Backward pass: Compute the gradient $g = \frac{\partial L}{\partial \theta} (\theta^{(e-1)}, D^{train})$
- 3. Step: Update the parameters: $\theta^{(e)} = \theta^{(e-1)} lr * g$

Important design decisions / hyperparameters

Initialization method?

Number of epochs? Or alternative way to decide to stop?

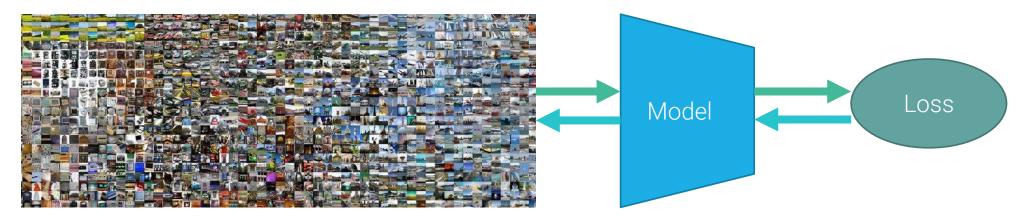
Learning rate *lr*?

Limits of gradient descent

$$L(\theta, D^{train}) = \sum_{i} L(\theta, (x^{(i)}, y^{(i)})) \Rightarrow \nabla_{\theta} L(\theta, D^{train}) = \sum_{i} \nabla_{\theta} L(\theta, (x^{(i)}, y^{(i)}))$$

The total gradient $\nabla_{\theta} L$ is computed as the sum of the gradients of the single training samples.

Think about training a linear model on ImageNet (1.3M training images...).



1.3M forward passes and 1.3M backward passes just to perform one (usually tiny) step

Batch gradient descent is an approximation

ImageNet is large...

but all the possible images of its 1000 classes are a much larger set



The gradient computed by gradient descent approximates the "true" gradient, even when computed on all available training data, as they are a (large, but not full) sample of the true population (i.e., all the possible images of its classes)

SGD - Stochastic Gradient Descent

$$\theta^* = argmin_{\theta \in \Theta} \sum_{i} L(\theta, (x^{(i)}, y^{(i)}))$$

A faster alternative to optimize a differentiable function is stochastic gradient descent.

0. (Randomly) initialize $\theta^{(0)}$

for
$$e = 0, ..., E - 1$$
 epochs

1. Randomly shuffle examples in D^{train}

for
$$i = 0, ..., N - 1$$

- 2. Forward pass: classify $x^{(i)}$ to get the predictions $\hat{y}^{(i)} = f(x^{(i)}; \theta^{(e*N+i)})$ and the loss $L(\theta^{(e*N+i)}, (x^{(i)}, y^{(i)})$
- 3. Backward pass: Compute the gradient $g = \frac{\partial L}{\partial \theta} (\theta^{(e*N+i)}, (x^{(i)}, y^{(i)}))$
- 4. Step: Update the parameters: $\theta^{(e*N+i+1)} = \theta^{(e*N+i)} lr * g$

One sample instead of the full dataset Sometimes this is also called "on-line" GD

Parameters updated after every forward+backward pass

SGD - Stochastic Gradient Descent with minibatches

A compromise: use a mini-batch of data of size B at each iteration instead of a single example. The number of parameter updates in each epoch will be $U = \left\lceil \frac{N}{B} \right\rceil$

0. (Randomly) initialize $\theta^{(0)}$

for
$$e = 0, ..., E - 1$$
 epochs

1. Randomly shuffle examples in D^{train}

for
$$u = 0, ..., U - 1$$

- 2. Forward pass: classify the examples $X^{(u)} = \{x^{(Bu)}, \dots, x^{(B(u+1)-1)}\}$ to get the predictions $\hat{Y}^{(u)} = \{\hat{y}^{(Bu)}, \dots, \hat{y}^{(B(u+1)-1)}\} = f(X^{(u)}; \theta)^{(e*U+u)}$ and the loss $L(\theta^{(e*U+u)}, (X^{(u)}, Y^{(u)}))$
- 3. Backward pass: Compute the gradient $g = \frac{\partial L}{\partial \theta} (\theta^{(e*U+u)}, (X^{(u)}, Y^{(u)}))$
- 4. Step: Update the parameters: $\theta^{(e*U+u+1)} = \theta^{(e*U+u)} lr * g$

B samples are processed simultaneously For B=1 we recover online SGD, for B=N batch gradient descent

Design decisions / hyperparameters

Initialization method? Number of epochs? Or how to decide to stop? Learning rate, i.e. step size? Mini-batch size?

Mini batches - tradeoffs

- Larger batches provide smoother estimations of the gradient, but with less than linear returns.
- o Larger batches better exploit parallel hardware, below a minimum size no gain in training time.
- o If examples in a batch are processed in parallel, memory requirements scale linearly with batch size.
- Usually power of 2 sizes (more suited for parallel hardware), typical values on-single GPUs is 16 to 256, but modern distributed training can use values up to 8,192 or 16,384 on multiple GPUs. [Goyal et al. 2018]
- Smaller batches may have a regularization effect and results in better generalization, at the cost of longer training time. [Smith et al., 2020]
- Usual rule of thumb: start with the largest power of 2 size that fits in the memory of your GPU.
 Experiment from there, if time allows.

How to compute gradients?

Gradients can be computed

- Numerically
 - Slow and approximate
 - But easy to implement
- Analytically, by exploiting the rules of calculus and, in particular, the chain rule.

$$\frac{d}{dx}f(g(x)) = f'(g(x))g'(x)$$

o Exact, but slow, tedious, and error prone. For the linear classifier, we get

$$\frac{\partial L}{\partial b_j} = \frac{\partial}{\partial b_j} - \log\left(\frac{\exp(s_j)}{\sum_{k=1}^C \exp(s_k)}\right) = \frac{\partial}{\partial b_j} - \log\left(\frac{\exp(w_j x + b_j)}{\sum_{k=1}^C \exp(s_k)}\right) = -\frac{\sum_{k=1}^C \exp(s_k)}{\exp(w_j x + b_j)}\left(\frac{\partial}{\partial b_j} \frac{\exp(w_j x + b_j)}{\sum_{k=1}^C \exp(s_k)}\right) = \cdots$$

Automatically, by automatic differentiation, e.g. with the backpropagation algorithm

What does a linear model learn on CIFAR10?

Accuracy about 38%

Let's use the template matching interpretation of a linear classifier to understand what the model is learning

It looks like the background color is the predominant feature used by the model

Moreover, one template cannot capture multiple appearances within one class, e.g. rotated cars, trucks, etc..

Distance between templates and images is a distance in input space.



What's next?

Learn more effective **representations**.

